



Department of Defense INSTRUCTION

NUMBER 5240.6

July 16, 1996

ASD(C3I)

SUBJECT: Counterintelligence (CI) Awareness and Briefing Program

References: (a) DoD Directive 5240.6, subject as above, February 26, 1986 (canceled)
(b) DoD Directive 5137.1, "Assistant Secretary of Defense for Command, Control, Communications and Intelligence," February 12, 1992
(c) DoD Directive 5240.2, "DoD Counterintelligence," June 6, 1983
(d) National Security Decision Directive No. 12, "Security and Awareness of Foreign Contracts," August 5, 1993
(e) through (v), see enclosure 1

1. REISSUANCE AND PURPOSE

This Instruction reissues reference (a) and pursuant to the responsibilities and authorities assigned to the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C3I)) in references (b) and (c), does the following:

- 1.1. Implements reference (d) in the Department of Defense.
- 1.2. Implements policy, responsibilities and procedures for reporting and investigating, and updates contacts by DoD personnel with any person who attempts to acquire by unauthorized means information related to the national defense.
- 1.3. Provides for the handling of other threat information affecting the security of DoD personnel, operations, resources, installations, and information to include intrusions into automated information systems.
- 1.4. Reaffirms the requirement that all DoD personnel receive periodic briefings,

not less frequently than every three years, on all threats posed by foreign intelligence and terrorist organizations.

1.5. References judicial or administrative sanctions for DoD personnel who fail to comply with the requirements of this Instruction.

1.6. Establishes reporting requirements to the Office of the Secretary of Defense for program oversight, evaluation, trend analysis, and profiling of foreign intelligence and terrorist activities.

1.7. Assigns to the three Military Department Counterintelligence (CI) Agencies the responsibility for implementing the investigative and operational aspects of the CI Awareness and Briefing Program for designated DoD Components that do not have the requisite organic CI capability.

2. APPLICABILITY AND SCOPE

This Instruction applies to:

2.1. The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Unified Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components").

2.2. Cleared personnel of DoD contractors for their briefing and reporting requirements, as specified under E.O. 12829 (reference (e)) (hereafter referred to collectively as "the DoD contractors").

3. DEFINITIONS

Terms used in this Instruction are defined in enclosure 2.

4. POLICY

It is DoD policy that:

4.1. Active and Reserve military personnel and DoD civilian employees are to report to an appropriate authority any contact information or circumstances that could pose a threat to the security of U.S. personnel, DoD resources, and classified national

security information (hereafter referred to as "classified information"), or unclassified controlled information under E.O. 12598, DoD Directive 5230.24, DoD 5400.7-R, and DoD Directive 5210.83 (references (f), (g), (h), and (i)). An appropriate DoD authority is the individual's security officer, supervisor, commander, or servicing CI agency. Similarly, cleared DoD contractors are to report to an appropriate authority any contact information or circumstances that could pose a threat to the security of U.S. personnel, DoD resources and classified information. An appropriate authority for DoD contractors is their Facility Security Officer, the Federal Bureau of Investigation, or other Federal authorities, to include the Defense Investigative Service (DIS) as required by DoD 5220.22-M (reference (j)), the terms of a classified contract, and U.S. law.

4.2. All DoD personnel shall receive a periodic briefing on the threats posed by foreign intelligence, foreign commercial enterprises, terrorists, computer intruders and unauthorized disclosures. This reinforces the requirements of DoD Directive 0-2000.12 (reference (k)) and reflects DoD personnel's responsibility to report any such information to an appropriate authority.

4.3. Judicial and/or administrative action may be taken when personnel fail to report such required information.

5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence shall:

5.1.1. Provide policy and direction for reporting and investigating, reportable incidents under section 6., below, and the NSDD 12 (reference (d)). Additionally, the ASD(C3I) shall designate and transfer CI Executive Agent assignments for DoD Components as made necessary by reorganizations or changing circumstances within the Department of Defense.

5.1.2. Ensure that the Director, Defense Intelligence Agency (DIA), shall:

5.1.2.1. Coordinate all information reported under this Instruction about military personnel assigned to the DIA with the appropriate Military Department CI Agency; coordinate all information reported about civilian employees with the FBI, in accordance with the MOA (reference (l)); and refer internal DIA security incidents that might lead to the arrest or prosecution of a DIA employee with the FBI or a Military Department CI Agency, as appropriate.

5.1.2.2. Establish policies and procedures to implement this Instruction within the DIA and in support of the Chairman of the Joint Chiefs of Staff.

5.1.2.3. Develop for DIA and the Chairman of the Joint Chiefs of Staff a briefing program on security, foreign intelligence, and terrorism awareness. Ensure that all DIA personnel are briefed periodically on the requirements to report the information, as specified in paragraphs 6.1.1. through 6.1.3., below.

5.1.2.4. Report annually to the ASD(C3I) the information specified in subsection 6.4., below.

5.1.2.5. Promptly report to the ASD(C3I) any significant CI investigative referrals made to the Military Department CI Agencies or FBI, and any significant cases investigated by DIA due to refusal by the Military Department CI Agencies or the FBI.

5.1.3. Ensure that the Director, DIS, shall:

5.1.3.1. Develop and submit recommended changes to the ASD(C3I) for DoD 5220.22-M (reference (j)), to implement this Instruction within cleared defense contractor facilities.

5.1.3.2. Coordinate CI information reported to the DIS during the conduct of its personnel security investigations and industrial security activities with the appropriate DoD CI Agency; coordinate all CI information covered by this Instruction about DoD contractor personnel and DoD civilian personnel employed in the United States with the FBI or Military Department CI Agencies, in accordance with the MOA (reference (l)); and refer internal DIS security incidents that might lead to the arrest or prosecution of a DIS employee with the FBI or the Military Department CI Agencies, as appropriate.

5.1.3.3. Establish policies and procedures to implement this program within DIS, and oversee its implementation by DoD contractors under DIS cognizance.

5.1.3.4. Ensure that all DIS personnel are briefed periodically on the requirements to report the information, as specified in paragraphs 6.1.1 through 6.1.3., below.

5.1.3.5. Report annually to the ASD(C3I) the information specified in subsection 6.4., below.

5.1.3.6. Promptly report to the ASD(C3I) any significant CI investigative referrals to the Military Department CI Agencies or FBI, and any significant cases investigated by DIS due to refusal by the Military Department CI Agencies or FBI.

5.2. The Director, National Reconnaissance Office, shall:

5.2.1. Coordinate all information reported under this Instruction about military personnel assigned to the National Reconnaissance Office (NRO) with the appropriate Military Department CI Agency; coordinate all information reported about civilian employees or contractor affiliates with the FBI, in accordance with the MOA (reference (1)); and refer internal NRO security incidents that might lead to the arrest or prosecution of a NRO employee with the FBI or a Military Department CI Agency, as appropriate.

5.2.2. Establish policies and procedures to implement this program within the NRO.

5.2.3. Provide for the awareness and briefing of NRO's military and civilian personnel and contractor affiliates on the threat and personal reporting responsibilities, as specified in paragraphs 6.1.1 through 6.1.3., below.

5.2.4. Report annually to the ASD(C3I) the information as in subsection 6.4., below.

5.2.5. Promptly report to the ASD(C3I) any significant CI investigative referrals to the Military Department CI Agencies or FBI, and any significant incidents investigated by NRO due to refusal by the Military Department CI Agencies or FBI.

5.3. The Director, National Security Agency, shall:

5.3.1. Coordinate all information reported under this Instruction about military personnel assigned to the National Security Agency (NSA) with the Military Department CI Agencies; coordinate all information reported about civilian employees or contractor affiliates with the FBI, in accordance with the MOA (reference (1)); and refer internal NSA security incidents that might lead to the arrest or prosecution of a NSA employee with the FBI or a Military Department CI Agency, as appropriate.

5.3.2. Establish policies and procedures to implement this program within the NSA.

5.3.3. Provide for the awareness and briefing of NSA's military and civilian personnel and contractor affiliates on the threat and personal reporting responsibilities, as specified in paragraphs 6.1.1. through 6.1.3., below.

5.3.4. Report annually to the ASD(C3I) the information in subsection 6.4., below.

5.3.5. Promptly report to the ASD(C3I) any significant CI investigative referrals to the Military Department CI Agencies or FBI, and any significant incidents investigated by NSA due to refusal by the Military Department CI Agencies or FBI.

5.4. The Secretaries of the Military Departments, shall:

5.4.1. Provide for the conduct, direction, management, coordination, and control of the CI Awareness and Briefing Program in their Departments in accordance with this Instruction.

5.4.2. Establish Military Department plans, programs, policies, and procedures to implement this program.

5.4.3. Provide for the awareness and briefing of their military and civilian personnel on the threat and personal reporting responsibilities specified in subsection 6.1., below.

5.4.4. Ensure that reported information, as specified in paragraphs 6.1.1. through 6.1.3., below, involving temporarily assigned military personnel, civilian employees, or DoD contactors, is provided to those individuals' parent DoD CI Agency.

5.4.5. Report annually to the ASD(C3I) the information in subsection 6.4., below.

5.4.6. Direct their respective Military Department CI Agencies to provide CI support to other DoD Components that do not have a CI capability, in accordance with the Executive Agent assignments in enclosure 3. Special agents of the Military Department CI Agencies will be on call to support a supported Component's request, and will utilize space and administrative support provided by the Military Department CI Agency at its field operating element closest to the supported Component. A supported DoD Component may establish and support a day office in the Component activity for use by special agents. The Military Department CI Agency will fund all costs associated with the special agent's CI activities. Analysis, reports, studies,

estimates, or publications generated on foreign intelligence services, their targets, methods of operation, personnel, activities, communications, funding, and support; international terrorism; and related security threats to DoD interests will be prepared, published, and disseminated using Military Department CI Agency resources. In its capacity as Executive Agency, the Military Department CI Agency will, as appropriate:

5.4.6.1. Assign a special agent(s) to receive CI issue referrals from a DoD Component Head or his or her designee.

5.4.6.2. Promulgate a Memorandum of Agreement or Understanding, in coordination with the DoD Component, specifying the tailored CI support it will provide.

5.4.6.3. Undertake the development of CI operations with the support of the DoD Component.

5.4.6.4. Conduct CI investigations in response to alleged offenses by DoD Component personnel.

5.4.6.5. Present CI awareness briefings to DoD Component personnel.

5.4.6.6. Provide threat analysis to the DoD Component Head or his or her designee.

5.4.6.7. Provide assistance in the referral of other CI matters to other DoD CI Agencies or the FBI and function as the DoD Component's liaison point for coordination of CI matters with other U.S. CI Agencies.

5.4.6.8. Periodically provide a report on current CI trends and threats, with emphasis on foreign intelligence service recruitment techniques, to the ASD(C3I), with copies to the other Military Department CI Agencies.

5.4.7. Promptly report to the ASD(C3I) any significant CI investigations initiated as a result of reporting under this Instruction and report any significant CI investigations involving DoD contractors to DIS.

5.5. The Under Secretary of Defense for Acquisition and Technology shall ensure that the Director, On-Site Inspection Agency, shall:

5.5.1. Coordinate all information reported under this Instruction about military personnel assigned to the OSIA with the Military Department CI Agencies;

coordinate all information reported about civilian employees or contractor affiliates with the FBI, in accordance with the MOA (reference (1)); and refer internal OSIA security incidents that might lead to the arrest or prosecution of a OSIA employee with the FBI or a Military Department CI Agency, as appropriate.

5.5.2. Establish policies and procedures to implement this program within the OSIA.

5.5.3. Provide for the awareness and briefing of their military and civilian personnel and contractor affiliates on the threat and personal reporting responsibilities, as specified in paragraphs 6.1.1. through 6.1.3., below.

5.5.4. Report annually to the ASD(C3I) the information as in subsection 6.4., below.

5.5.4. Promptly report to the ASD(C3I) any significant CI investigative referrals to the Military Department CI Agencies or the FBI, and any significant incidents investigated by OSIA due to refusal by the Military Department CI Agencies or the FBI.

5.6. The Heads of the DoD Components (except the Secretaries of the Military Departments; the Director, Defense Intelligence Agency; the Director, Defense Investigative Service; the Director, National Reconnaissance Office; the Director, NSA; and Director, On-Site Inspection Agency) shall, if the Head of a DoD Component is unsure as to where to refer reported CI information, the nearest Military Department CI Agency office should be contacted for guidance.

5.6.1. Refer to the applicable Military Department CI Agency any CI information involving military personnel assigned to their Components for investigation and disposition.

5.6.2. Refer reported CI information involving civilian employees employed by their Component in the United States to their servicing Military Department CI Agency and, when overseas, to the Military Department responsible for providing administrative and logistical support.

5.6.3. Establish policies and procedures to implement this program in their Components.

5.6.4. Provide for the awareness and briefing of their military and civilian personnel on the threat and personal reporting responsibilities, as specified in

paragraphs 6.1.1. through 6.1.3., below.

5.6.5. Report annually to the ASD(C3I) the information in subsection 6.4., below, and apprise the CI Executive Agent of the reporting.

6. PROCEDURES

6.1. Reporting Requirements

6.1.1. DoD personnel who have had contact, as described below, are required to report that contact, either verbally or in writing, to their security officer, supervisor, commander, or servicing DoD CI Agency for action. That report may support CI reporting and trend analysis, investigative, operational and other exploitation possibilities. Contacts for reporting purposes are defined as:

6.1.1.1. Contact with an individual (regardless of nationality) that suggests to the DoD employee that a foreign interest intelligence or terrorist organization may have targeted him or her for possible intelligence exploitation.

6.1.1.2. A request by anyone (regardless of nationality) for illegal or unauthorized access to classified or unclassified controlled information.

6.1.1.3. Contact with a known or suspected intelligence officer from any country.

6.1.1.4. Contact with a foreign diplomatic establishment, whether in the United States or abroad, for personal or official reasons. Certain DoD personnel in positions designated as “sensitive” by their DoD Component may also be required to apprise their commanders or supervisors in advance of the nature and reason for contacting a foreign diplomatic establishment.

6.1.2. Additionally, DoD personnel who have information about activities pertaining to espionage, terrorism, unauthorized technology transfer, sabotage, sedition, subversion, spying, treason, unauthorized release of classified or unclassified controlled information, or unauthorized intrusions into automated information systems are required to report that information to their security officer, supervisor, or commander, who must then report the information to the servicing DoD CI Agency for action. Information may also be reported by individuals directly to the servicing DoD CI Agency. Each DoD Component shall establish a program requiring reporting of the following information:

6.1.2.1. Activities for planned, attempted, actual, or suspected espionage, terrorism, unauthorized technology transfer, sabotage, sedition, subversion, spying, treason or other intelligence activities against the Department of Defense, other U.S. facilities, organizations, or U.S. citizens.

6.1.2.2. Information indicating the deliberate compromise or unauthorized release of classified or unclassified controlled information, attempted or contemplated or completed by DoD personnel, with the intention of conveying such documents, information or material to any unauthorized persons.

6.1.2.3. Unauthorized intrusions into U.S. automated informations systems, whether classified or unclassified; unauthorized transmissions of classified or unclassified controlled information over commercial on-line computer services and telephones, whether originated from work or from home.

6.1.3. Continuing official and unofficial contacts with foreign government interests also may be reportable under separate reporting procedures, such as those concerning DoD attaches or arms control negotiators. The DoD Components must identify to their employees, contractors, and to the ASD(C3I) additional requirements for reporting contacts beyond those enunciated in paragraphs 6.1.1. through 6.1.3., above.

6.2. Awareness and Briefing Requirements. Each DoD Component shall establish a program to ensure the personnel for whom the Component is responsible are aware of the threats to personnel, material, and information, and educated about the personal responsibilities in combatting and reporting those threats. That program shall:

6.2.1. Enable personnel to identify reportable situations and incidents promptly.

6.2.2. Ensure prompt, proper response to, and timely reporting of, such information to appropriate authority.

6.2.3. Present the general threat and focus on specific threat information and reporting responsibilities that are current and relevant; and are reasonably tailored to the nature, level, functions, prior knowledge and responsibilities of the receiving individuals and to the type of employing organization and its mission, activities, and location.

6.2.4. Have a variety of awareness and education means, including live and

recorded presentations, written and visual materials, and other sources.

6.2.5. Provide briefings on threat and personal responsibilities at or near the time of initial entry or hire and at least at 36-month intervals, thereafter, with more frequent briefings, as needed. Briefings may also cover basic security tenets and principles such as the use of unsecured phone lines and classified on-line computer services, classification process, declassification procedures and the authorized disclosure of classified material to foreign representatives.

6.2.6. Employ other means between briefings to maintain a continual awareness of the threat and personal responsibilities sufficient to ensure the program's objectives in paragraphs 6.2.1. and 6.2.2., above, are met.

6.2.7. Use the servicing Military Department CI Agency, where feasible, as the source of those briefings and material or use the Component as a primary point of coordination on their content and application.

6.3. Sanctions. DoD or contractor personnel who fail to report information required by this Instruction may be subject to judicial and/or administrative action under applicable law and regulations, including the Uniform Code of Military Justice, 10 U.S.C. 801-940 (reference (m)), and other applicable sections of the United States Code.

6.4. Analysis of Reports. The following categories of information shall be used in making reports based on data required by paragraphs 6.1.1., 6.1.2., and 6.1.3. above to ensure uniformity between DoD Components:

6.4.1. Category I. Includes any reported incident of contact or request for information in which foreign intelligence service involvement is confirmed.

6.4.2. Category II. Includes any reported incident of contact or request for information in which some evidence suggests foreign intelligence service involvement (based on the name used by the perpetrator and/or elicitor, physical description, method of operation, or the type of information requested).

6.4.3. Category III. Includes any reported solicitation of classified or unclassified controlled information not made through official channels or under authorized procedures, in which foreign intelligence service involvement is considered to be remote. ("Category IV" has been deleted from this Instruction.)

6.4.4. Category V. Includes any reported information about international or

domestic terrorist groups and/or activities that pose a potential threat to the security of DoD or other U.S. personnel, resources, or facilities.

6.4.5. Category VI. Includes any reported incident of deliberate compromise of classified information by DoD personnel to an unauthorized person or entity.

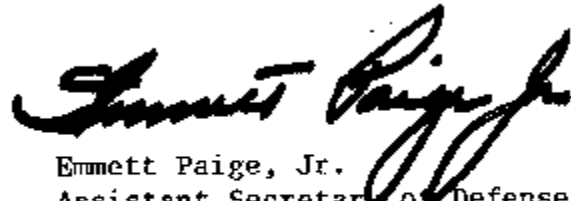
6.5. Oversight Requirements. For oversight and program evaluation, the servicing DoD CI Agencies, in conjunction with the DoD Components, shall maintain a record of the incidents and information reported in each category in paragraphs 6.4.1. through 6.4.5., above. An annual report, advising of the number of reports by category, paragraphs 6.4.1. through 6.4.5. for the preceding fiscal year, shall be provided by DoD CI Agencies to the Director of Counterintelligence and Security Programs, Office of the ASD(C3I), by November 1.

7. INFORMATION REQUIREMENTS

The reporting requirements in paragraphs 6.4.1. through 6.4.5., above, are exempt from licensing in accordance with DoD 8910.1-M, paragraph 6.4.8. (reference (n)).

8. EFFECTIVE DATE

This Instruction is effective immediately.



Emmett Paige, Jr.
Assistant Secretary of Defense
(Command, Control, Communications
and Intelligence)

Enclosures - 3

1. References
2. Definitions
3. List of CI Executive Agents for Defense Agencies and OSD

E1. ENCLOSURE 1

REFERENCES, continued

- (e) Executive Order 12829, "National Industrial Security Program," January 6, 1993
- (f) Executive Order 12958, "Classified National Security Information," April 17, 1995
- (g) DoD Directive 5230.24, "Distribution Statements on Technical Documents," March 18, 1987
- (h) DoD 5400.7-R, "DoD Freedom of Information Act Program," October 1990, authorized by DoD Directive 5400.7, "DoD Freedom of Information Act Program," May 13, 1988
- (i) DoD Directive 5210.83, "Unclassified Controlled Nuclear Information," November 15, 1991
- (j) DoD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)," January 1995 authorized by DoD Directive 5220.22, December 8, 1980
- (k) DoD Directive 0-2000.12, "DoD Combatting Terrorism Program," August 27, 1990
- (l) Memorandum of Agreement between the Department of Defense Counterintelligence Agencies and the Federal Bureau of Investigation, April 5, 1979
- (m) Section 801-940, Chapter 47, of title 10, United States Code, "Uniform Code of Military Justice"
- (n) DoD 8910.1-M, "DoD Procedures for Management of Information Requirements," November 1986, authorized by DoD Directive 8910.1, "DoD Procedures for Management of Information Requirements," June 11, 1993
- (o) DoD Directive 5230.25, "Withholding of Unclassified Technical Data from Public Disclosure," November 6, 1984
- (p) Sections 792-799, Chapter 37, of title 18, United States Code, "Espionage and Censorship"
- (q) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992
- (r) Sections 2151 and 2156, Chapter 105, of title 18, United States Code, "Sabotage"
- (s) Sections 2381-2391, Chapter 177, of title 18, United States Code, "Treason, Sedition, and Subversive Activities"
- (t) Section 2401 of title 50, United States Code, "Export Regulation"
- (u) Section 2751 of title 22, United States Code, "Arms Export Control"
- (v) Section 1030, of title 18, United States Code, "Fraud and Related Activity In Connection with Computers"

E2. ENCLOSURE 2

DEFINITIONS

E2.1.1. Counterintelligence (CI) Investigation. Includes inquiries and other activities undertaken to determine whether a particular person is acting for, or on behalf of, a foreign power for espionage, treason, spying, sedition, subversion, sabotage, assassinations, international terrorist activities, and actions to neutralize such acts.

E2.1.2. CI Operation. Actions taken against foreign intelligence services to counter espionage and other clandestine intelligence activities damaging to the national security.

E2.1.3. Classified National Security Information. (Also referred to as Classified Information.) Information that has been determined to require protection against unauthorized disclosure and is marked to indicate its classified status when in document form, pursuant to E.O. 12958 (reference (f)).

E2.1.4. Contact. Any form of meeting, association, or communication, in person, by radio, telephone, letter or other means, regardless of who started the contact or whether it was for social, official, private, or other reasons.

E2.1.5. Counterintelligence (CI). Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.

E2.1.6. Espionage. As in 18 U.S.C. 792-798, (reference (p)):

E2.1.6.1. Espionage is the act of obtaining, delivering, transmitting, communicating, or receiving information about the national defense with an intent or reason to believe that the information may be used to the injury of the United States or to the advantage of any foreign nation. The offense of espionage applies during war or peace.

E2.1.6.2. Section 793 of reference (p) makes it an offense to gather, with the requisite intent or belief, national defense information, by going on, entering, flying over, or obtaining access by any means to any installation or place used by the United States for national defense. The method of gathering that information is immaterial.

E2.1.6.3. Anyone who lawfully or unlawfully is entrusted with or otherwise has possession of, access to, or control over information about national defense that he or she has reason to believe could be used against the United States or to the advantage of any foreign nation, and willingly communicates or transmits, or attempts to communicate or transmit, such information to any person not entitled to receive it, is guilty of espionage.

E2.1.6.4. Anyone entrusted with or having lawful possession or control of information about national defense, who through gross negligence permits the same to be lost, stolen, abstracted, destroyed, removed from its proper place of custody, or delivered to anyone in violation of that trust, is guilty of violating the espionage statutes.

E2.1.6.5. If two or more persons conspire to commit and one of them commits an overt act in furtherance of such conspiracy, all members of the conspiracy may be punished for violation of the espionage statutes.

E2.1.6.6. The espionage statutes are not intended to cover classified military information shared with foreign governments and international organizations when there is a clearly defined benefit to the United States and only where authorized by officials designated under DoD Directive 5230.11 (reference (q)) and only where all requirements of that Directive are met.

E2.1.7. Foreign Diplomatic Establishment. Any embassy, consulate, or interest section representing a foreign country.

E2.1.8. Foreign Interest. Any foreign government, agency of a foreign government, or representative of a foreign government; any form of business enterprise or legal entity organized, chartered or incorporated under the laws of any country other than the United States, or its possessions and trust territories, and any person who is not a citizen or national of the United States.

E2.1.9. Military Department CI Agency and DoD CI Agency. The Military Department CI Agencies include Army Counterintelligence; the Naval Criminal Investigative Service; and the Air Force Office of Special Investigations. The DoD CI Agencies include the foregoing, plus the CI elements of DIA, DIS, NRO, NSA, and OSIA (which have internal CI support and/or limited CI responsibilities).

E2.1.10. Sabotage. An act or acts with the intent to injure or interfere with, or obstruct the national defense of a country by willfully injuring, destroying, or

attempting to destroy any national defense or war material, premises, or utilities to include human or natural resources 18 U.S.C. 2151 (reference (r)).

E2.1.11. Sedition. An act or acts intending to cause the overthrow or destruction of the Government of the United States by force or violence, or by the assassination of any U.S. Government officer. These acts include conspiracy, knowingly or willingly advocating, abetting, advising, or teaching the duty, necessity, desirability, or propriety of overthrowing or destroying by force or violence the U.S. Government under 18 U.S.C. 2384-2385 (reference (s)).

E2.1.12. Spying. In time of war, any person who, acting clandestinely or under false pretense, obtains or seeks to obtain information with the intent to convey it to a hostile party under 10 U.S.C. 906 (reference (m)).

E2.1.13. Subversion. An act or acts inciting military or civilian personnel of the Department of Defense to violate laws, disobey lawful orders or regulations, or disrupt military activities with the willful intent to interfere with, or impair the loyalty, morale, discipline, of the military forces of the United States under 18 U.S.C. 2381-2391 (reference (s)).

E2.1.14. Technology Transfer. The unauthorized export of controlled technical information, data, and/or material to a foreign interest pursuant to 50 U.S.C. 2401 (reference (t)) and 22 U.S.C. 2751 (reference (u)).

E2.1.15. Terrorism. The calculated use of violence or threat of violence to inculcate fear intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

E2.1.16. Treason. One who, owing allegiance to the United States, levies war against the United States or adheres to its enemies, giving them aid and comfort within the United States or elsewhere. It also includes one who, having knowledge of the commission of treason, conceals and does not, as soon as may be, report it 18 U.S.C. 2381-2391 (reference (s)).

E2.1.17. Unauthorized Intrusions and Unauthorized Discussions on Computer Services. One who accesses a computer without authorization or exceeds authorized access, and by means of such conduct obtains information that has been determined to require protection for reason of national defense or foreign relations, or any restricted data with the intent or reason to believe that such information is to be used to the injury of the United States, or to the advantage of any foreign nation under 18 U.S.C.

1030 (reference (v)); or, one having unauthorized possession of information relating to the national defense that the possessor has reason to believe could be used to the injury of the United States or to the advantage of a foreign nation, willfully communicates or transmits the same to any person not entitled to receive it over commercial on-line computer services under 18 U.S.C. 793 (reference (p)).

E2.1.18. Unclassified Controlled Information. Information other than classified information that has been determined by appropriate authority to require particular protection measures. For example, information that bears a distribution limitation statement from DoD Directive 5230.24 (reference (g)); information that is being marked "For Official Use Only," in accordance with DoD 5400.7-R, Chapter IV (reference (h)); unclassified controlled nuclear information under DoD Directive 5210.83 (reference (i)); or information withheld from public disclosure, in accordance with DoD Directive 5230.25 (reference (o)).

E2.1.19. Unofficial Contact. Contact not specifically required, in accordance with job responsibilities.

E3. ENCLOSURE 3LIST OF CI EXECUTIVE AGENTS FOR DEFENSE AGENCIES AND OFFICE OF
THE SECRETARY OF DEFENSE¹

	Defense Components	Executive Agent
1.	Advance Research Projects Agency	Naval Criminal Investigative
2.	Ballistic Missile Defense Organization	Air Force Office of Special Investigations
3.	Central Imagery Office	Air Force Office of Special Investigations
4.	Defense Commissary Agency	Army Counterintelligence
5.	Defense Contract Audit Agency	Army Counterintelligence
6.	Defense Finance and Accounting Service	Naval Criminal Investigative Service
7.	Defense Information Systems Agency	Naval Criminal Investigative Service
8.	Defense Legal Services Agency	Air Force Office of Special Investigations
9.	Defense Logistics Agency	Air Force Office of Special Investigations
10.	Defense Mapping Agency	Army Counterintelligence
11.	Defense Special Weapons Agencies	Army Counterintelligence
12.	Defense Security Assistance Agency	Air Force Office of Special Investigations
13.	Defense Technology Security Administration	Naval Criminal Investigative Service
14.	Office of the Secretary of Defense	Air Force Office of Special Investigations

¹ The Defense Intelligence Agency, Defense Investigative Service, National Reconnaissance Office, National Security Agency, and On-Site Inspection Agency have internal CI support and/or limited CI responsibilities.